RCA PU030087 AC+AA US 2002/012433 Ref AA corresponds

CITED BY APPLICANT

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 842 055**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **02 08481**

(51) Int Cl[7] : H 04 L 12/417

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 05.07.02.

(30) Priorité :

(43) Date de mise à la disposition du public de la demande : 09.01.04 Bulletin 04/02.

(56) Liste des documents cités dans le rapport de recherche préliminaire : *Se reporter à la fin du présent fascicule*

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *NORTEL NETWORKS LIMITED* — CA.

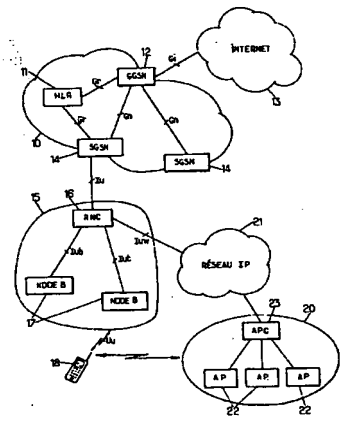
(72) Inventeur(s) : STOJANOVSKI SASO, STEER DAVID G et FAUCONNIER DENIS.

(73) Titulaire(s) :

(74) Mandataire(s) : CABINET PLASSERAUD.

(54) PROCEDE POUR CONTROLER L'ACCES A UN SYSTEME CELLULAIRE DE RADIOCOMMUNICATION A TRAVERS UN RESEAU LOCAL SANS FIL, ET ORGANE DE CONTROLE POUR LA MISE EN OEUVRE DU PROCEDE.

(57) Le système de radiocommunication cellulaire a un réseau d'accès radio (15) comportant des stations de base et un organe de contrôle (16) auquel est relié un réseau local sans fil (20). Pour contrôler l'accès d'un terminal bi-mode (18) au système cellulaire à travers le réseau local sans fil, on exécute les étapes suivantes: authentifier le terminal auprès du système cellulaire par l'intermédiaire du réseau d'accès radio; allouer au terminal un jeton d'authentification; transmettre le jeton alloué de l'organe de contrôle au terminal par l'intermédiaire du réseau d'accès radio; transmettre le jeton alloué et un identifiant du terminal de l'organe de contrôle à un serveur d'authentification accessible par l'intermédiaire du réseau sans fil; et authentifier le terminal auprès du réseau sans fil en vérifiant que le terminal possède le jeton transmis au serveur d'authentification.



FR 2 842 055 - A1

PROCEDE POUR CONTROLER L'ACCES A UN SYSTEME CELLULAIRE DE RADIOCOMMUNICATION A TRAVERS UN RESEAU LOCAL SANS FIL, ET ORGANE DE CONTROLE POUR LA MISE EN ŒUVRE DU PROCEDE

La présente invention concerne les techniques d'accès aux réseaux cellulaires depuis des terminaux radio. Elle vise plus particulièrement le contrôle d'accès à un ou plusieurs systèmes cellulaires de radiocommunication à travers un réseau local sans fil.

Des réseaux locaux sans fil, ou WLAN ("Wireless Local Area Networks"), permettent aujourd'hui aux utilisateurs de terminaux appropriés de disposer d'accès à haut débit à des services de télécommunication. Il a été proposé d'associer de tels réseaux locaux à des systèmes cellulaires étendus, afin de procurer aux abonnés de ces systèmes cellulaires une grande capacité de débit dans des zones déterminées ("hot spots").

Ce genre d'association peut concerner divers types de WLAN et divers types de systèmes cellulaires. A des fins d'illustration et sans que ceci soit limitatif, on s'intéressera plus particulièrement dans la suite à des WLAN de type IEEE 802.11 normalisés par l'IEEE ("Institute of Electrical and Electronics Engineers"), et à des systèmes cellulaires de troisième génération de type UMTS ("Universal Mobile Telecommunication System") normalisés par l'organisation 3GPP ("3rd Generation Partnership Project").

La plupart des systèmes cellulaires actuels, notamment les systèmes UMTS, comportent d'une part un réseau cœur et d'autre part un ou plusieurs réseau d'accès radio. Le réseau cœur comporte des commutateurs maillés entre eux, appelés GSN ("GPRS Support Nodes"), ainsi que divers serveurs utilisés notamment pour la gestion des abonnés du système (HLR, "Home Location Register"). Le réseau d'accès le plus courant des systèmes UMTS est appelé UTRAN ("UMTS Terrestrial Radio Access Network"). Il se compose d'organes de contrôle appelés RNC ("Radio Network Controller") et de stations de base appelées "nodes B" réparties sur la zone de couverture du réseau d'accès et contrôlées chacune par l'un des RNC.

Pour associer une technologie WLAN à un tel système cellulaire, il a

été proposé un schéma d'intégration à couplage faible entre les deux technologies. De façon typique, il est alors prévu une passerelle entre le WLAN et un HLR du réseau cœur du système cellulaire.

La présente invention se rapporte plutôt à des schémas d'intégration à couplage étroit entre les deux technologies, ce qui permet aux utilisateurs des stations IEEE 802.11 de bénéficier d'une grande partie des services procurés par l'infrastructure cellulaire.

La figure 1 montre une architecture que l'on peut obtenir lorsqu'on applique un tel schéma d'intégration. Les commutateurs du réseau cœur 10 communiquent entre eux par une interface normalisée dite *Gn*, et avec le HLR 11 par l'intermédiaire d'une interface dite *Gr*. On distingue les GGSN 12 ("Gateway GSN") qui servent de passerelles avec des réseaux externes 13 tels que l'Internet par exemple, et les SGSN 14 ("Serving GSN") qui sont reliés à l'UTRAN à travers une interface dite *Iu*.

L'UTRAN 15 comporte un certain nombre de RNC 16 qui sont chacun reliés à un SGSN du réseau cœur à travers l'interface *Iu* (un seul RNC est représenté sur la figure 1). Chaque RNC contrôle un ou plusieurs node B 17 à travers une interface dite *Iub*. L'interface radio entre un node B 17 et un terminal UMTS 18 (UE, "User Equipment") est appelée *Uu*.

Dans le schéma d'intégration illustré par la figure 1, le RNC 16 est en outre relié à un WLAN 20 par l'intermédiaire d'un réseau routé 21 basé sur le protocole IP. Le WLAN 20 comporte un ou plusieurs point d'accès 22, appelés AP ("Access Point") dans la terminologie IEEE. S'il y a plusieurs AP 22, ils sont typiquement supervisés par un système de distribution 23 pouvant prender la forme d'un contrôleur de point d'accès (APC, "Access Point Controller").

Un terminal bi-mode UMTS / IEEE 802.11 est capable de communiquer par radio avec un node B 17 mais aussi avec un AP 22.

Ce schéma de couplage étroit permet de réutiliser les concepts UMTS de qualité de service, de sécurité et de mobilité pour les utilisateurs accédant au système par l'intermédiaire du WLAN 20. Il permet également à ses utilisateurs d'accéder à tous les services UMTS, notamment de localisation.

Compte tenu du parc relativement important d'AP de type IEEE 802.11 déjà installés, il est souhaitable que le schéma de couplage étroit impose un minimum d'exigences au niveau de ces AP. C'est la raison pour laquelle la pile de protocole UMTS sur l'interface RNC/WLAN (appelée ici interface *Iuw*) est avantageusement construite par dessus la pile UDP/IP habituelle dans les WLAN, comme illustré par la figure 2.

La figure 2 montre des piles de protocole utilisées pour les échanges entre un UE bi-mode 18 et le RNC 16 par l'intermédiaire du réseau local sans fil 20. A l'intérieur du WLAN 20, la couche physique est conforme aux spécifications IEEE 802.11 sur l'interface radio et, par exemple, aux spécifications IEEE 802.3 sur l'interface filaire entre l'AP 22 et l'APC 23. Le protocole de couche liaison est LLC, tel que spécifié dans la norme IEEE 802.2. La figure 2 montre également la couche de protocole IP utilisée pour router les informations entre le RNC 16 et le terminal 18 par l'intermédiaire du WLAN 20. Dans l'exemple représenté, cette couche IP est aussi incluse dans l'APC 23, qui constitue un routeur. L'APC, lorsqu'il est présent, pourrait cependant jouer un simple rôle de passerelle de couche 2. Le protocole de couche transport utilisé est UDP ("User Datagram Protocol"). Les paquets UDP/IP servent alors à transporter des informations relevant de canaux logiques UMTS.

Ainsi, tous les services UMTS relevant de la couche 2 ou plus sont disponibles pour un terminal mobile 18 accédant au système par l'intermédiaire du WLAN 20. En particulier, des ports UDP spécifiques du RNC 16 et du terminal 18 sont utilisés pour des canaux dédiés de trafic (DTCH, "Dedicated Trafic CHannel") ou de contrôle (DCCH, "Dedicated Control CHannel"), dont les blocs de transport sont construits et traités par une instance du protocole UMTS MAC-d ("Medium Access Control – dedicated channels"). D'autres ports UDP sont utilisés pour les canaux communs UMTS, en particulier pour les canaux logiques descendants de type BCCH ("Broadcast Control CHannel") et PCCH ("Paging Control CHannel") et pour les canaux logiques montants et descendants de type CCCH ("Common Control CHannel").

Dans les réseaux IEEE 802.11 classiques, il existe deux modes de

contrôle d'accès des stations à l'interface radio :

- un mode en système ouvert, dans lequel les stations ne sont pas authentifiées : lorsqu'une station capte la balise IEEE 802.11 émise par un AP, elle émet une requête d'authentification à laquelle l'AP répond toujours positivement avant que la station s'associe à l'AP;
- un mode sécurisé dans lequel le WLAN s'assure que la station détient une clé partagée pour l'authentifier et lui permettre de s'associer.

Dans un schéma d'intégration de la technologie WLAN à un système cellulaire étendu, avec des abonnés en itinérance ("roamers"), il n'est pas réaliste de faire partager une clé secrète à tous les abonnés du système cellulaire susceptibles d'y accéder par l'intermédiaire d'un WLAN déterminé. Il est donc naturel de fonctionner en système ouvert au niveau du WLAN et d'assurer l'authentification des terminaux au sein du système cellulaire. Mais ceci pose un certain nombre de difficultés.

Tout d'abord, les opérateurs UMTS proposant des accès WLAN souhaitent typiquement restreindre l'accès en mode IEEE 802.11 aux seuls clients potentiels, c'est-à-dire aux utilisateurs ayant des terminaux bi-mode WLAN / UMTS. En particulier, il est souhaitable de filtrer les stations IEEE 802.11 qui ne sont pas compatibles UMTS. Cependant, lorsque le WLAN fonctionne en système ouvert, toute station IEEE 802.11 est capable de s'associer auprès d'un AP et d'obtenir une adresse IP auprès d'un serveur d'allocation dynamique d'adresses, en général selon le protocole DHCP ("Dynamic Host Configuration Protocol"). Même si les stations non compatibles UMTS ne peuvent pas aller plus loin et accéder au RNC, il en résulte une consommation de ressources inappropriée dans le WLAN, notamment en termes d'adressage IP.

De plus, il serait relativement facile pour une personne malveillante d'implémenter la pile de protocole UMTS à partir de la couche MAC dans une station IEEE 802.11. Une station ainsi bricolée pourrait aisément établir une connexion du protocole RRC ("Radio Resource Control") avec le RNC 16 puis diriger des requêtes de service répétitives vers le réseau cœur 10.

En outre, il se peut que plusieurs zones desservies par des WLAN

IEEE 802.11 se chevauchent. Dans un tel cas, il est souhaitable de pouvoir indiquer au terminal auprès de quel(s) point(s) d'accès il devrait s'associer.

Il se peut également qu'un même WLAN 20 soit interfacé avec des RNC appartenant à des systèmes cellulaires d'opérateurs différents. Dans ce cas, il est judicieux de pouvoir désigner au terminal le RNC avec lequel il convient d'établir la connexion RRC.

Comme le canal BCCH portant les informations système utiles aux échanges avec l'infrastructure UMTS est un canal de diffusion, l'adresse IP de destination que spécifie le RNC dans les datagrammes transportant ces informations BCCH doit être reconnue par les terminaux comme étant une adresse de diffusion. Pour cela, on utilise typiquement l'adresse IP de "diffusion limitée" (1111 ... 111). Cependant, les datagrammes envoyés à cette adresse ne sont diffusés que dans le voisinage immédiat de l'émetteur. En conséquence, s'il se trouve que le RNC n'appartient pas au même sous-réseau IP que les AP, le RNC doit plutôt utiliser une adresse de diffusion à l'intérieur du sous-réseau IP dont relève le ou les AP pertinents afin d'atteindre l'interface radio, c'est-à-dire une adresse IP ayant le format : (< IP Subnet Prefix > 111 ... 111). Mais l'utilisation d'une adresse de diffusion dans un sous-réseau IP crée un autre problème. Etant donné que le terminal 18 n'a généralement pas d'adresse IP prédéfinie (il en obtient une au moyen d'une transaction DHCP), il ne connaît pas le préfixe de sous-réseau IP (IP Subnet Prefix) de sorte qu'il peut être incapable de détecter l'adresse IP de diffusion et donc de recevoir les informations système UMTS.

En 2001, l'IEEE a publié la norme IEEE 802.1X qui traite le contrôle d'accès à des réseaux locaux en améliorant l'authentification des terminaux au moyen d'un serveur centralisé. Cette norme est applicable à tous les réseaux locaux de la série 802, notamment IEEE 802.3, IEEE 802.5 et IEEE 802.11. L'authentification IEEE 802.1X est basée sur un secret que l'usager partage avec le serveur et non avec l'AP. Les messages d'authentification sont conformes à un protocole EAP ("Extensible Authentication Protocol") et transportés dans des trames EAPOL ("EAP Over LAN") sur l'interface radio et, par exemple, dans des trames RADIUS sur le réseau filaire.

Un but de la présente invention est de faciliter le contrôle d'accès des terminaux bi-modes à un système cellulaire de radiocommunication à travers un réseau local sans fil, en limitant l'incidence des problèmes exposés ci-dessus.

L'invention propose ainsi un procédé pour contrôler l'accès à au moins un système cellulaire de radiocommunication à travers un réseau local sans fil, le système cellulaire ayant un réseau d'accès radio comportant des stations de base et un organe de contrôle auquel est relié ledit réseau sans fil. Selon l'invention, le procédé comprend les étapes suivantes:

- authentifier un terminal auprès du système cellulaire par l'intermédiaire du réseau d'accès radio;
- allouer audit terminal un jeton d'authentification;
- transmettre le jeton alloué de l'organe de contrôle au terminal par l'intermédiaire du réseau d'accès radio;
- transmettre le jeton alloué et un identifiant du terminal de l'organe de contrôle à un serveur d'authentification accessible par l'intermédiaire dudit réseau sans fil; et
- authentifier le terminal auprès du réseau sans fil en vérifiant que le terminal possède le jeton transmis audit serveur d'authentification.

Un terminal s'entend ici comme un équipement d'usager capable de communiquer avec un système cellulaire, et aussi avec un réseau local sans fil. La plupart des systèmes actuels considèrent des terminaux formés en associant un module d'identité d'abonné (SIM, "Subscriber Identity Module") à un appareil non spécifique d'un abonnement. Le cas le plus représentatif est alors celui où l'authentification porte sur l'abonnement, c'est-à-dire qu'elle met en jeu le SIM. Selon les méthodes employées, l'authentification peut éventuellement requérir la saisie d'un code secret ou d'un mot de passe de la part de l'usager. On peut aussi envisager que l'authentification porte sur l'appareil, voire conjointement sur l'appareil et sur le SIM. D'autre part, l'authentification pourrait aussi porter sur des terminaux ne possédant pas la notion de SIM.

Certains des paramètres essentiels à l'accès d'un terminal par

l'intermédiaire d'un WLAN ne sont fournis à ce terminal qu'après authentification auprès du système cellulaire. L'authentification WLAN n'est pas assurée exclusivement au niveau des AP, mais fait intervenir un serveur d'authentification accessible des terminaux par le WLAN et qui reçoit les informations utiles de l'organe de contrôle. Dans le cas typique où le WLAN est de technologie IEEE 802.11, cette authentification peut être effectuée en mode IEEE 802.1X.

Dans une réalisation simple, le jeton d'authentification est utilisé comme un mot de passe temporaire, dont la validité est couplée avec un identifiant d'usager temporaire. Dans une autre réalisation, le jeton est utilisé comme une clef de chiffrement temporaire, avec laquelle le terminal chiffre un challenge proposé par le serveur. L'authentification peut aussi être mutuelle, c'est-à-dire que non seulement le serveur authentifie le terminal, mais aussi le terminal est capable d'authentifier le serveur, afin d'éviter de se raccorder à un éventuel WLAN malveillant. Par "jeton d'authentification", on entend ainsi un ensemble de paramètres d'authentification (mot de passe, clef de chiffrement temporaire, etc.) suivant le protocole d'authentification utilisé. Comme le standard IEEE 802.1X, l'invention n'est pas limitée quant aux protocoles d'authentification.

Dans une réalisation de l'invention, l'allocation du jeton d'authentification est effectuée par l'organe de contrôle. Dans un certain nombre de systèmes cellulaires, tels que l'UMTS, l'échange initial entre le terminal et l'organe de contrôle (RNC) comporte la transmission par le terminal d'une liste de caractéristiques de celui-ci. Dans le cas d'un terminal bi-mode UMTS / WLAN, ces caractéristiques comprennent l'indication de ce caractère bi-mode. L'allocation du jeton d'authentification par le RNC peut alors être conditionnée par le fait que la liste transmise par le terminal indique une telle capacité bi-mode.

L'organe de contrôle transmet avantageusement le jeton d'authentification au terminal avec de l'information d'identification se rapportant au réseau local sans fil. Ceci permet au terminal de savoir auprès de quel WLAN il est habilité à s'associer. Cette information d'identification peut être

sélectionnée par l'organe de contrôle sur la base d'une localisation du terminal dans le réseau d'accès radio.

Cette localisation résulte par exemple de la station de base du réseau d'accès radio par l'intermédiaire de laquelle s'établit le dialogue terminal / organe de contrôle. Certains systèmes cellulaires, par exemple l'UMTS, offrent des techniques de localisation du terminal fonctionnant avec une précision meilleure que la granularité d'une cellule. Une de ces techniques repose sur l'utilisation du GPS ("Global Positioning System"), auquel cas la précision de la localisation est de quelques mètres.

Lorsque le réseau local sans fil est relié à l'organe de contrôle à travers un réseau IP, le jeton d'authentification est avantageusement transmis au terminal avec de l'information d'adressage dans ce réseau IP. Cette information d'adressage peut avantageusement comporter :

- une adresse de diffusion de sous-réseau IP employée par l'organe de contrôle pour diffuser des informations système par l'intermédiaire du WLAN;
- une adresse IP du serveur d'authentification dans le réseau IP;
- l'adresse IP de l'organe de contrôle.

Ces différentes informations d'adressage permettent d'obtenir une très grande souplesse de mise en œuvre du couplage étroit entre un ou plusieurs systèmes cellulaires et un ou plusieurs WLAN.

Un autre aspect de la présente invention se rapporte à un organe de contrôle pour un réseau d'accès radio d'un système cellulaire de radiocommunication, comprenant:

- des moyens d'interface avec au moins une station de base du système cellulaire;
- des moyens d'interface avec un réseau local sans fil;
- des moyens d'allocation d'un jeton d'authentification à un terminal authentifié auprès du système cellulaire par l'intermédiaire du réseau d'accès radio;
- des moyens de transmission au terminal du jeton alloué par l'intermédiaire du réseau d'accès radio; et

- des moyens de transmission du jeton alloué et d'un identifiant du terminal à un serveur d'authentification accessible par l'intermédiaire dudit réseau sans fil, de telle sorte que le terminal soit authentifié auprès du réseau sans fil par vérification de ce que le terminal possède le jeton transmis audit serveur d'authentification.

D'autres particularités et avantages de la présente invention apparaîtront dans la description ci-après d'exemples de réalisation non limitatifs, en référence aux dessins annexés, dans lesquels :

- la figure 1, précédemment commentée, est un schéma d'ensemble d'un système UMTS auquel on a intégré un WLAN selon un schéma de couplage étroit;
- la figure 2, précédemment commentée, est un diagramme montrant des piles de protocoles utilisées pour l'accès au système UMTS à travers le WLAN;
- la figure 3 est un schéma synoptique montrant diverses entités d'un réseau IP utilisé entre le WLAN à un ou plusieurs systèmes UMTS; et
- les figures 4A et 4B sont des diagrammes illustrant des exemples d'échanges de messages intervenant conformément à l'invention pour contrôler l'accès d'un terminal bi-mode au système illustré par les figures 1 et 3.

La figure 3 montre des éléments du réseau IP 21 de la figure 1, utilisés dans un mode de réalisation de l'invention. Ce réseau peut comprendre un ou plusieurs routeurs 30 pour acheminer les datagrammes IP. Le WLAN 20 considéré ici correspond à ce qu'on appelle un ESS ("Extended Service Set") dans le jargon IEEE, c'est-à-dire qu'il s'étend sur les zones de couverture de plusieurs AP 22 appartenant au même sous-réseau IP. L'APC 23 peut aussi jouer un rôle de routeur IP, comme illustré par la figure 2.

Dans l'exemple considéré sur la figure 3, le réseau IP 21 permet de mettre en liaison le WLAN 20 avec deux UTRAN 15, appartenant par exemple à deux opérateurs cellulaires différents A, B. Il y a alors deux RNC 16 présentant l'interface *Iuw* vers le même WLAN.

Le réseau IP 21 est pourvu d'un serveur DHCP 31 pour assurer

l'allocation dynamique d'adresses IP à des stations IEEE 802.11 en liaison avec les AP 22. Cette allocation dynamique est effectuée de façon connue en utilisant le protocole DHCP décrit dans la RFC 2131 publiée en mars 1997 par l'IETF ("Internet Engineering Task Force").

Le réseau IP 21 est en outre équipé d'un serveur d'authentification 32 pour effectuer l'authentification des stations IEEE 802.11 conformément à la norme IEEE 802.1X précitée.

Conformément à l'invention, l'authentification d'un terminal bi-mode 18 est effectuée en deux temps pour lui permettre d'accéder au système à travers un WLAN: d'abord auprès du système cellulaire 10 (HLR), puis auprès du WLAN 20.

Dans la première phase, le terminal 18 dialogue avec le système cellulaire par l'intermédiaire du réseau d'accès 15, c'est-à-dire que les échanges avec le RNC 16 passent par un node B 17, comme illustré par la figure 4A.

Une première étape 40 peut consister en l'établissement d'une connexion RRC entre l'UE 18 et le RNC 16. Le protocole RRC est décrit en détail dans la spécification technique 3G TS 25.331, V3.3.0, "RRC Protocol Specification" publiée en juin 2000 par le 3GPP. La procédure d'établissement de connexion RRC est décrite dans la section 8.1.3 de cette spécification.

Une fois la connexion RRC établie, l'étape suivante 41 comporte l'authentification du terminal 18 par le réseau cœur 10.

La façon d'authentifier un terminal UMTS est décrite dans la section 6.3 de la spécification technique 3G TS 33.102, V3.5.0, "Security Architecture", publiée en juillet 2000 par le 3GPP. Le SGSN 14 interroge d'abord le HLR 11 en indiquant l'identité (IMSI, "International Mobile Subscriber Identity") du terminal 18. La réponse du HLR comprend un ou plusieurs vecteurs d'authentification comprenant plusieurs paramètres utiles à l'authentification et à l'échange de clés de chiffrement avec le terminal. Le SGSN utilise un vecteur pour tester le terminal dans un message "*Authentification_and_ciphering_request*". Le terminal utilise alors les données d'abonnement qu'il détient ainsi qu'un algorithme d'authentification pour générer une réponse

"*Authentification_and_ciphering_response*" qu'il retourne au SGSN. Celui-ci vérifie alors la validité de la réponse par rapport au vecteur utilisé pour authentifier ou non le terminal 18.

Cette procédure d'authentification peut être employée dans divers contextes de gestion de mobilité faisant intervenir le SGSN (voir section 3.4.2 de la spécification technique 3G TS 24.008, V3.4.1, "Core Network Protocols – Stage 3", publiée en juillet 2000 par le 3GPP). Dans l'exemple représenté sur la figure 4A, le contexte est celui d'une inscription du terminal mobile auprès du réseau cœur ("IMSI attach").

De façon connue, le RNC 16 peut obtenir une liste de caractéristiques du terminal mobile 18 ayant établi la connexion RRC. C'est l'objet de l'étape 42 indiquée sur la figure 4A. Le RNC interroge le terminal dans un message "*UE_capability_enquiry*", auquel le terminal répond en indiquant ses caractéristiques dans le message "*UE_capability_information*", comme décrit dans les sections 8.1.6 et 8.1.7 de la spécification 3G TS 25.331 précitée.

Les caractéristiques du terminal peuvent aussi avoir été fournies lors de l'établissement de la connexion RRC, notamment dans le message "*Connection_Setup_Complete*" de l'étape 40. Dans ce cas, l'étape 42 n'est pas nécessaire.

Dans le cas qui nous intéresse ici, le terminal 18 indique sa capacité bi-mode dans le message "*Connection_Setup_Complete*" ou "*UE_capability_information*", de telle sorte que le RNC 16 sait qu'il s'agit d'un terminal compatible IEEE 802.11.

Comme le RNC 16 sait par ailleurs qu'il est relié à un ou plusieurs WLAN 20 par l'interface *Iuw*, il ménage la possibilité que le terminal 18 accède au système par l'intermédiaire d'un tel WLAN.

Pour cela, il alloue au terminal bi-mode 18 un jeton d'authentification qui permettra à ce dernier de s'authentifier auprès du WLAN 20. Le jeton d'authentification consiste en un mot de passe ou une autre forme de secret partagé. Le RNC le transmet d'une part au terminal bi-mode 18 et d'autre part au serveur d'authentification 32. Le jeton d'authentification n'a qu'une validité temporaire, fixée par le RNC.

La transmission du jeton au terminal 18 peut notamment être effectuée dans des champs disponibles du message "*Security_mode_command*" du protocole RRC (section 8.1.12 de la spécification 3G TS 25.331), auquel le terminal répond par un message "*Security_mode_complete*" après avoir pris en compte les paramètres de sécurité stipulés par le RNC (échange 43 sur la figure 4A).

Le jeton d'authentification est transmis au serveur 32, avec une identité du terminal concerné, dans un ou plusieurs datagrammes UDP/IP acheminés dans le réseau 21. L'identité du terminal peut être l'IMSI ou de préférence le TMSI ("Temporary Mobile Subscriber Identity") alloué au terminal au cours de la procédure d'inscription 41.

Dans une réalisation préférée de l'invention, le message ("*Security_mode_command*" ou autre) par lequel le RNC 16 fournit le jeton d'authentification au terminal 18 comporte également les éléments d'information suivants :

- ESS ID : identifiant du WLAN 20, permettant au terminal de savoir s'il est habilité à s'inscrire auprès d'un WLAN donné;
- IP Subnet Prefix : préfixe de sous-réseau IP utilisé dans le WLAN, c'est-à-dire que tous les terminaux qui s'y associent obtiennent des adresses IP commençant par ce préfixe. Ce préfixe permet de connaître l'adresse IP, de la forme < IP Subnet Prefix > 111 ... 111, employée par le RNC 16 pour diffuser les informations système du BCCH;
- RNC IP @ : adresse IP du RNC 16 dans le réseau 21, permettant au terminal de communiquer avec le RNC à travers le WLAN 20 suivant la connexion RRC établie; et
- Auth. Server IP @ : adresse IP du serveur d'authentification 32, pour que le terminal procède à son authentification au sein du WLAN 20.

Il est possible d'ajouter à ces éléments d'information l'adresse IP du serveur DHCP 31 auquel le terminal s'adresse pour obtenir une adresse IP allouée dynamiquement.

Il est à noter que le RNC 16 peut avantageusement tenir compte de la localisation du terminal dans l'UTRAN 15 pour sélectionner les paramètres ci-

dessus. Par exemple, il pourra désigner un WLAN, par le paramètre ESS ID, lorsque le terminal est en liaison avec un node B 17 proche de la zone de couverture de ce WLAN.

Il est également possible que le RNC 16 soit relié à plusieurs WLAN, auquel cas un ou plusieurs paramètres ESS ID sont fournis au terminal en fonction de sa localisation. Il est notamment possible d'avoir plusieurs picocellules WLAN dans une seule macrocellule UMTS (cellule parapluie). Le node B peut alors être proche de plus d'un WLAN. Grâce aux techniques de localisation UMTS, le RNC peut connaître la position du mobile de manière plus précise que la granularité d'une macrocellule.

La figure 4B illustre une séquence de messages pouvant intervenir pour autoriser l'accès au système cellulaire, à travers le WLAN 20, d'un terminal bi-mode 18 ayant reçu un jeton d'authentification.

La balise radio IEEE 802.11 diffusée par un AP 22 inclut l'identifiant ESS ID. Lorsque cette balise est captée par le terminal ayant reçu cette valeur ESS ID avec son jeton d'authentification, il peut procéder à son association 44 avec l'AP puis entamer la procédure d'authentification auprès du WLAN.

Comme indiqué en traits interrompus sur la figure 4B, le terminal est d'ores et déjà en mesure de recevoir les informations système du RNC par l'intermédiaire du WLAN 20, étant donné qu'il a connaissance de l'adresse IP sur laquelle celui-ci diffuse le canal BCCH (< IP Subnet Prefix > 111 ... 111).

L'authentification du terminal auprès du WLAN 20 (étape 45 de la figure 4B) est effectuée selon la méthode IEEE 802.1X, c'est-à-dire par un dialogue entre le terminal 18 et le serveur d'authentification 32 selon le protocole EAP, l'AP 22 assurant les traductions de format EAPOL / RADIUS. La séquence de messages 45 est détaillée sur la figure 4B.

Lorsque l'authentification est un succès, l'étape suivante 46 est la transaction DHCP entre le terminal 18 et le serveur 31 pour fournir une adresse IP dynamique au terminal.

Une fois qu'il a obtenu cette adresse IP, le terminal peut dialoguer avec le RNC 16 sur un canal commun CCCH transposé sur des ports UDP/IP. Dans

l'exemple représenté sur la figure 4B, ce dialogue 47 consiste en une mise à jour de la cellule d'affectation du terminal (procédure "*Cell Update*" de la section 8.3.1 de la spécification 3G TS 25.331).

Il est à noter que l'adresse IP du serveur d'authentification 32 peut ne pas être transmise explicitement au terminal par le RNC si l'identité d'utilisateur employée pour l'authentification IEEE 802.1X est codée au format IMSI-in-NAI, c'est-à-dire sous la forme 0IMSI@realm. La raison en est que la partie "realm" identifie implicitement le serveur d'authentification. Le terminal 18 peut alors s'adresser à un serveur de nom de domaine (DNS, "Domain Name Server") pour récupérer l'adresse IP du serveur 32 avant de procéder à son authentification.

La transmission explicite de cette adresse IP par le RNC présente l'avantage de faire l'économie de cette transaction DNS.

Le procédé d'authentification précédemment décrit est applicable dans le cas général où plusieurs opérateurs UMTS peuvent partager le même WLAN 20, comme dans la configuration illustrée par la figure 3.

Le procédé est également applicable dans le cas où le même WLAN serait impliqué à la fois dans un schéma de couplage étroit et dans un schéma de couplage faible. L'adresse du serveur d'authentification, ou la partie "realm" de l'identifiant IMSI-in-NAI, permet alors d'acheminer les messages d'authentification vers le serveur adéquat (par exemple un serveur local pour le couplage étroit et un serveur distant pour le couplage faible).

REVENDICATIONS

1. Procédé pour contrôler l'accès à au moins un système cellulaire de radiocommunication à travers un réseau local sans fil (20), le système cellulaire ayant un réseau d'accès radio (15) comportant des stations de base (17) et un organe de contrôle (16) auquel est relié ledit réseau sans fil, le procédé comprenant les étapes suivantes:

- authentifier un terminal (18) auprès du système cellulaire par l'intermédiaire du réseau d'accès radio;
- allouer audit terminal un jeton d'authentification;
- transmettre le jeton alloué de l'organe de contrôle au terminal par l'intermédiaire du réseau d'accès radio;
- transmettre le jeton alloué et un identifiant du terminal de l'organe de contrôle à un serveur d'authentification (32) accessible par l'intermédiaire dudit réseau sans fil; et
- authentifier le terminal auprès du réseau sans fil en vérifiant que le terminal possède le jeton transmis audit serveur d'authentification.

2. Procédé selon la revendication 1, dans lequel l'allocation du jeton d'authentification est effectuée par l'organe de contrôle (16).

3. Procédé selon la revendication 2, dans lequel des terminaux adaptés au système cellulaire transmettent chacun une liste respective de caractéristiques à l'organe de contrôle (16), et dans lequel l'allocation d'un jeton d'authentification à un terminal (18) authentifié auprès du système cellulaire est effectuée à condition que la liste transmise par ledit terminal indique une capacité d'accès au réseau sans fil (20).

4. Procédé selon l'une quelconque des revendications précédentes, dans lequel le jeton d'authentification est alloué de manière temporaire au terminal (18).

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel le jeton d'authentification est transmis au terminal (18) avec de l'information d'identification se rapportant au réseau local sans fil (20).

6. Procédé selon la revendication 5, dans lequel le réseau local sans fil (20) auquel se rapporte ladite information d'identification est sélectionné sur la base d'une localisation du terminal (18) dans le réseau d'accès radio (15).

7. Procédé selon l'une quelconque des revendications précédentes, dans lequel le réseau sans fil (20) est relié à l'organe de contrôle (16) à travers un réseau IP (21).

8. Procédé selon la revendication 7, dans lequel le jeton d'authentification est transmis au terminal (18) avec de l'information d'adressage dans ledit réseau IP (21).

9. Procédé selon la revendication 8, dans lequel ladite information d'adressage comporte une adresse de diffusion de sous-réseau IP employée par l'organe de contrôle (16) pour diffuser des informations système par l'intermédiaire du réseau local sans fil (20).

10. Procédé selon la revendication 8 ou 9, dans lequel le serveur d'authentification (32) est un serveur dudit réseau IP (21), et dans lequel ladite information d'adressage comporte une adresse IP du serveur d'authentification.

11. Procédé selon l'une quelconque des revendications 8 à 10, dans lequel ladite information d'adressage comporte une adresse IP de l'organe de contrôle (16).

12. Organe de contrôle pour un réseau d'accès radio (15) d'un système cellulaire de radiocommunication, comprenant:

- des moyens d'interface avec au moins une station de base (17) du système cellulaire;
- des moyens d'interface avec un réseau local sans fil (20);

- des moyens d'allocation d'un jeton d'authentification à un terminal (18) authentifié auprès du système cellulaire par l'intermédiaire du réseau d'accès radio;
- des moyens de transmission au terminal du jeton alloué par l'intermédiaire du réseau d'accès radio; et
- des moyens de transmission du jeton alloué et d'un identifiant du terminal à un serveur d'authentification (32) accessible par l'intermédiaire dudit réseau sans fil, de telle sorte que le terminal soit authentifié auprès du réseau sans fil par vérification de ce que le terminal possède le jeton transmis audit serveur d'authentification.

13. Organe de contrôle selon la revendication 12, comprenant des moyens pour recevoir une liste respective de caractéristiques d'un terminal adapté au système cellulaire, et dans lequel les moyens d'allocation d'un jeton d'authentification à un terminal (18) authentifié auprès du système cellulaire sont activés à condition que la liste transmise par ledit terminal indique une capacité d'accès au réseau sans fil (20).

14. Organe de contrôle selon la revendication 12 ou 13, dans lequel le jeton d'authentification est alloué de manière temporaire au terminal (18).

15. Organe de contrôle selon l'une quelconque des revendications 12 à 14, dans lequel le jeton d'authentification est transmis au terminal (18) avec de l'information d'identification se rapportant au réseau local sans fil (20).

16. Organe de contrôle selon la revendication 15, dans lequel le réseau local sans fil (20) auquel se rapporte ladite information d'identification est sélectionné sur la base d'une localisation du terminal (18) dans le réseau d'accès radio (15).

17. Organe de contrôle selon l'une quelconque des revendications 12 à 16, dans lequel les moyens d'interface avec le réseau local sans fil (20) comprennent une interface IP.

18. Organe de contrôle selon la revendication 17, dans lequel le jeton d'authentification est transmis au terminal (18) avec de l'information d'adressage IP.

19. Organe de contrôle selon la revendication 18, dans lequel ladite information d'adressage comporte un préfixe de sous-réseau IP employé pour diffuser des informations système par l'intermédiaire du réseau local sans fil (20).

20. Organe de contrôle selon la revendication 18 ou 19, dans lequel ladite information d'adressage comporte une adresse IP du serveur d'authentification (32).

21. Organe de contrôle selon l'une quelconque des revendications 18 à 20, dans lequel ladite information d'adressage comporte une adresse IP de l'organe de contrôle (16).

FIG.1.

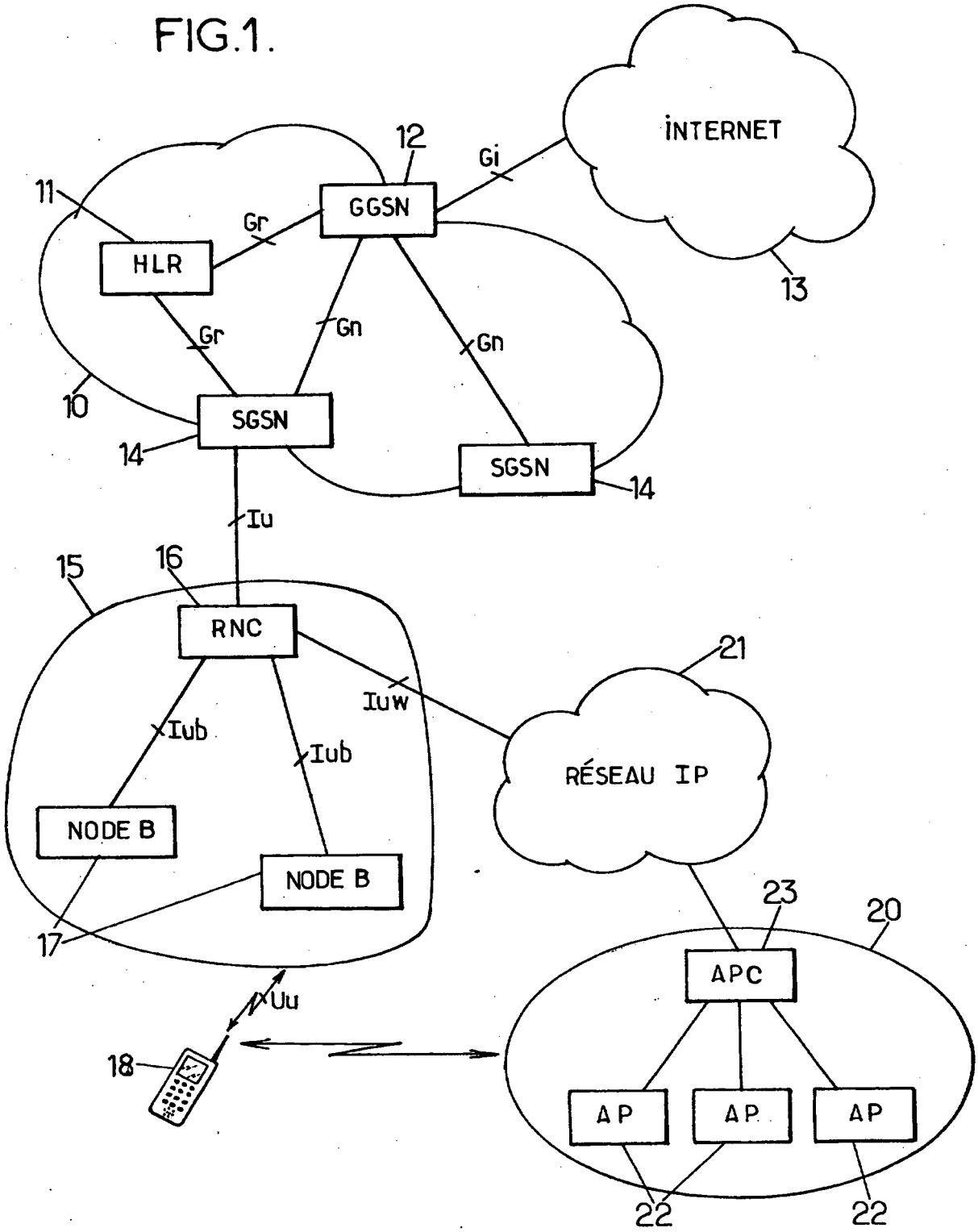

INTERNET
12
Gi
11
GGSN
Gr
HLR
13
Gr
Gn
Gn
10
SGSN
14
SGSN
14
Iu
15
16
RNC
21
Iuw
Iub
Iub
RÉSEAU IP
NODE B
NODE B
17
23
20
APC
Uu
18
AP
AP
AP
22
22

FIG.2.

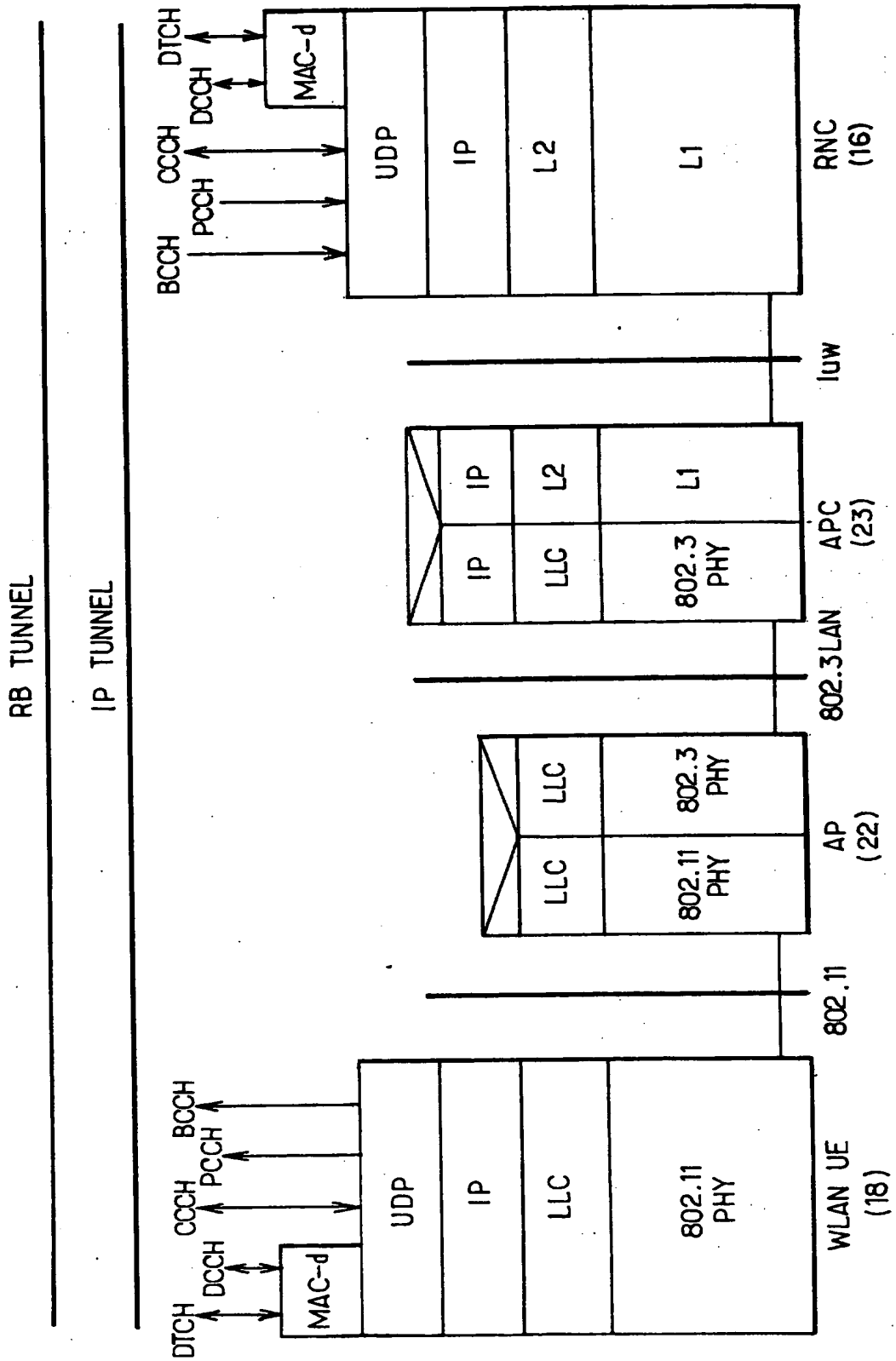

RB TUNNEL
IP TUNNEL
DTCH
DCCH
CCCH
PCCH
BCCH
MAC-d
UDP
IP
LLC
802.11 PHY
WLAN UE (18)
802.11
AP (22)
802.3LAN
APC (23)
802.3 PHY
L1
L2
Iuw
RNC (16)

FIG.3.

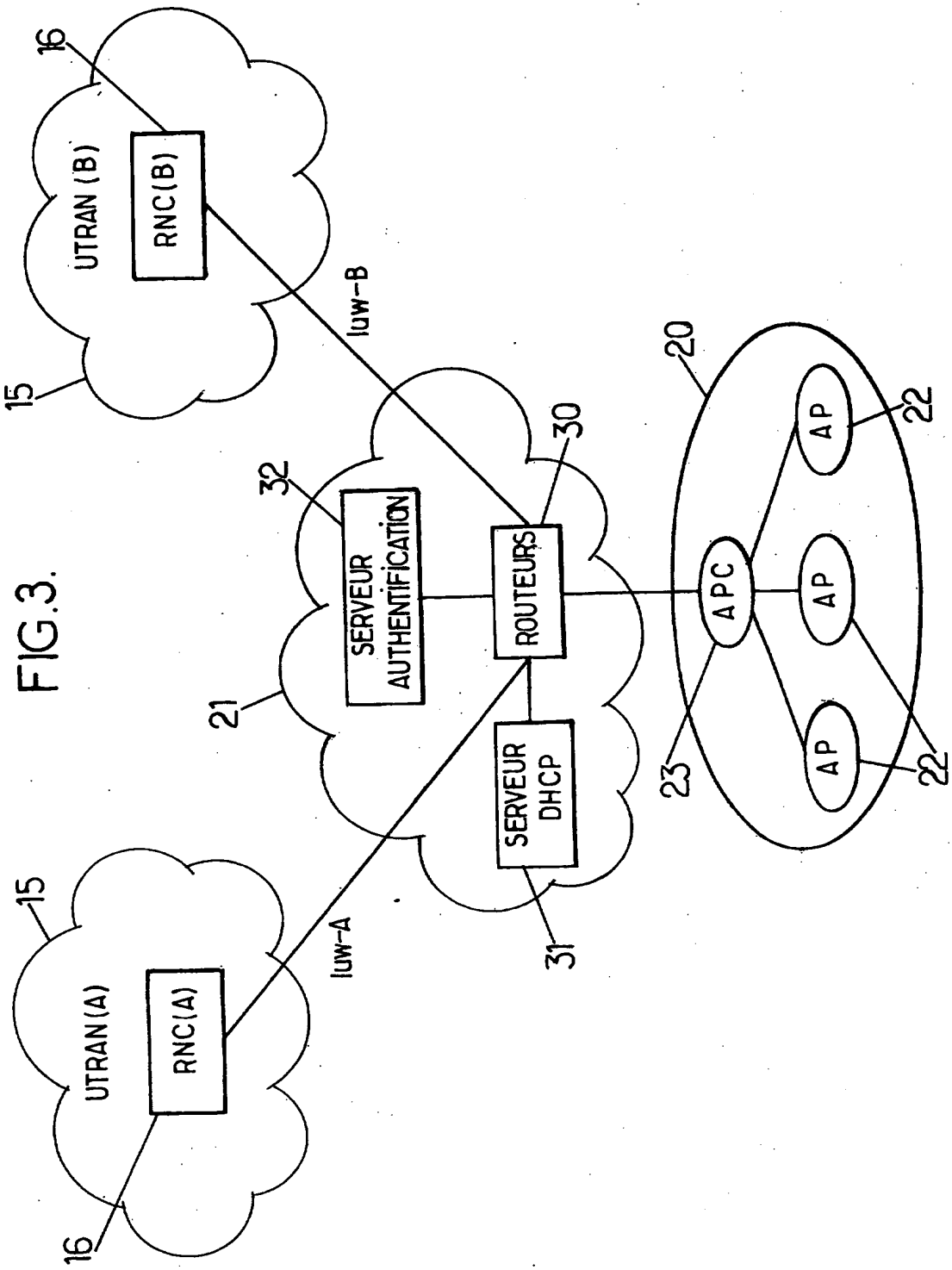

UTRAN (B)
RNC(B)
16
15
Iuw-B
UTRAN(A)
RNC(A)
15
16
Iuw-A
SERVEUR AUTHENTIFICATION
32
ROUTEURS
30
SERVEUR DHCP
31
21
20
APC
AP
AP
AP
22
22
23

FIG.4A.

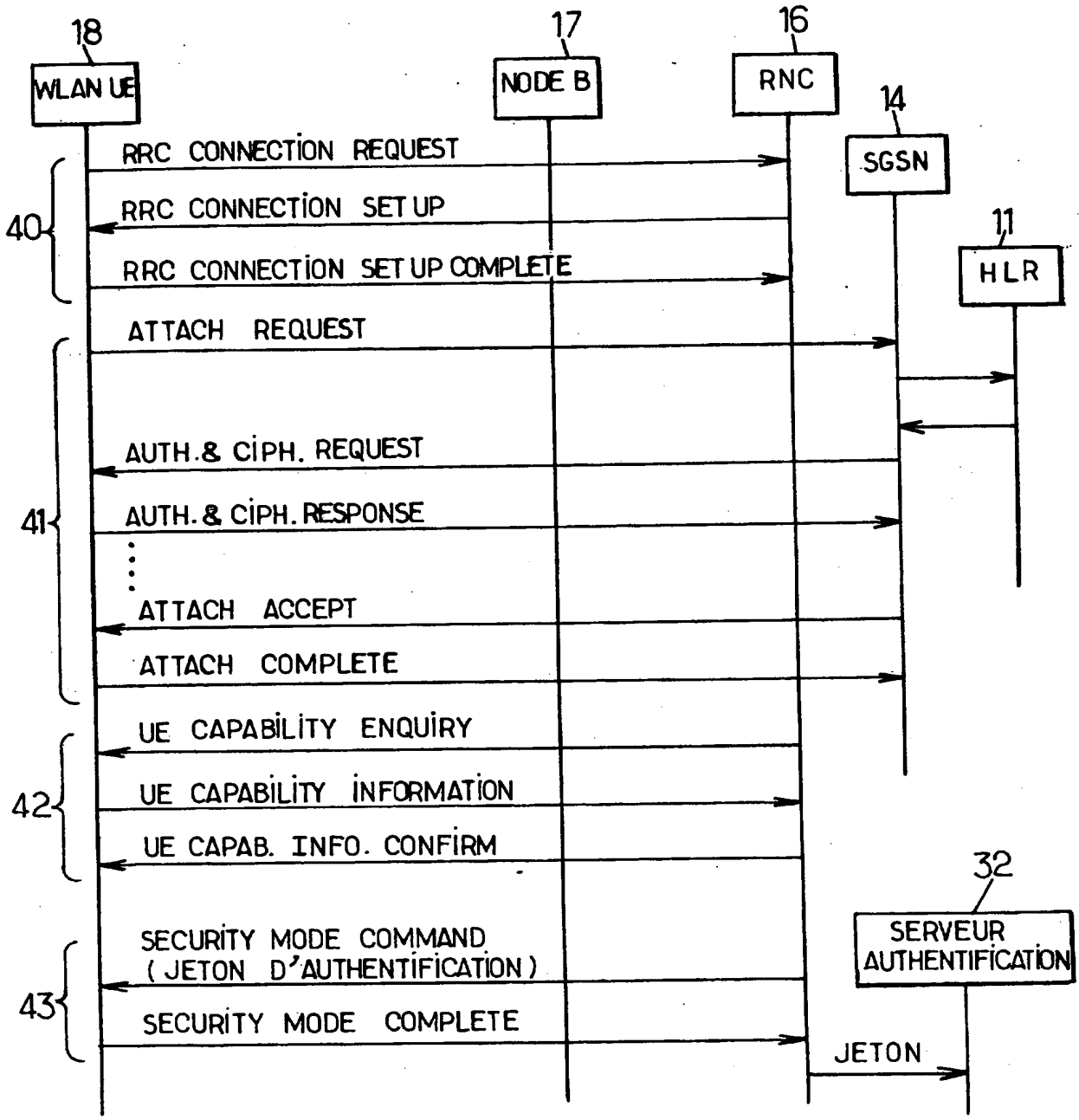
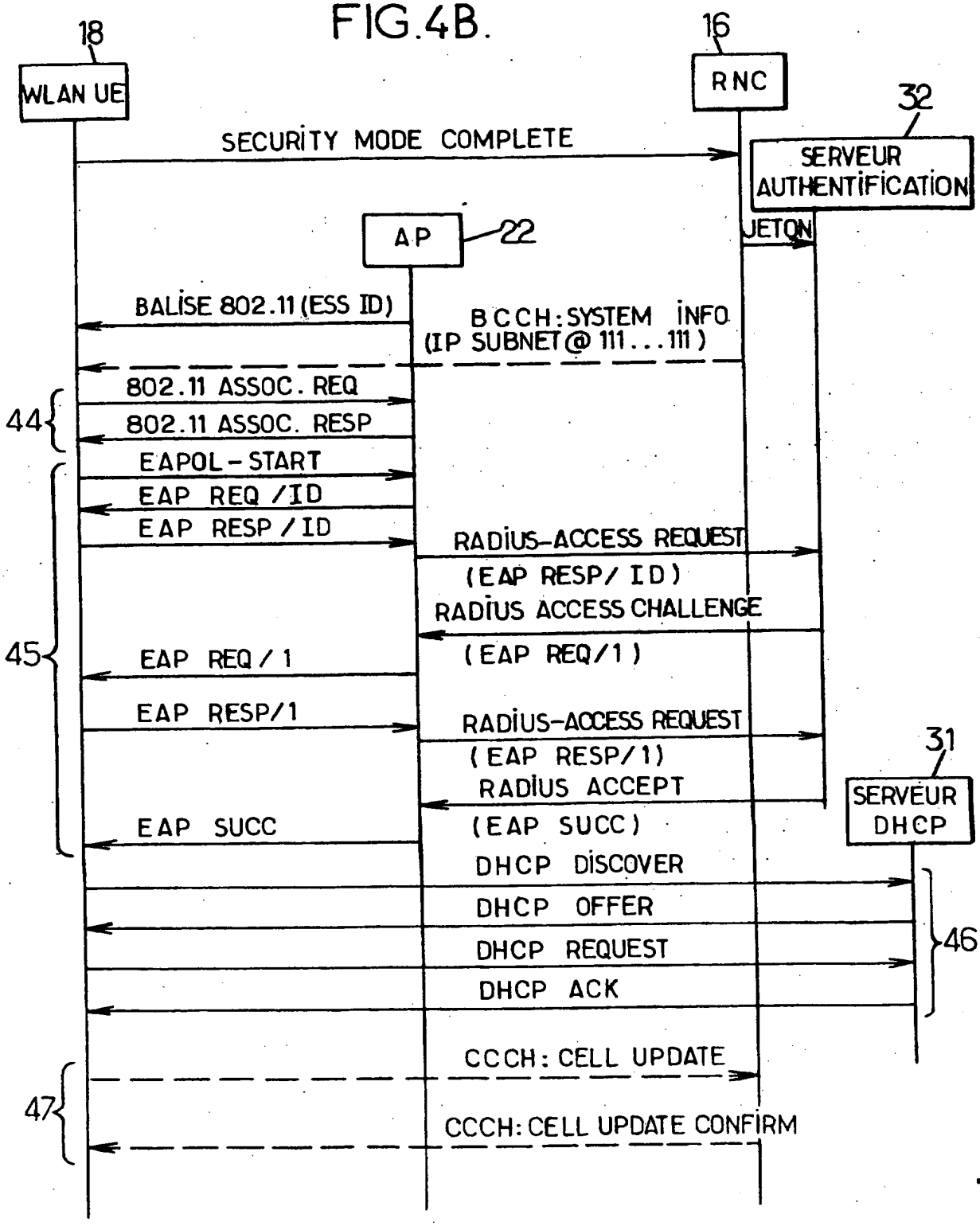

18
WLAN UE
17
NODE B
16
RNC
14
SGSN
11
HLR
32
SERVEUR AUTHENTIFICATION
RRC CONNECTION REQUEST
RRC CONNECTION SET UP
RRC CONNECTION SET UP COMPLETE
ATTACH REQUEST
AUTH. & CIPH. REQUEST
AUTH. & CIPH. RESPONSE
ATTACH ACCEPT
ATTACH COMPLETE
UE CAPABILITY ENQUIRY
UE CAPABILITY INFORMATION
UE CAPAB. INFO. CONFIRM
SECURITY MODE COMMAND
(JETON D'AUTHENTIFICATION)
SECURITY MODE COMPLETE
JETON
40
41
42
43

FIG.4B.


18
WLAN UE
16
RNC
32
SERVEUR AUTHENTIFICATION
SECURITY MODE COMPLETE
AP
22
JETON
BALISE 802.11 (ESS ID)
BCCH: SYSTEM INFO (IP SUBNET@ 111...111)
802.11 ASSOC. REQ
802.11 ASSOC. RESP
44
EAPOL-START
EAP REQ /ID
EAP RESP / ID
RADIUS-ACCESS REQUEST
(EAP RESP/ ID)
RADIUS ACCESS CHALLENGE
45
EAP REQ / 1
(EAP REQ/1)
EAP RESP/1
RADIUS-ACCESS REQUEST
(EAP RESP/1)
RADIUS ACCEPT
31
SERVEUR DHCP
EAP SUCC
(EAP SUCC)
DHCP DISCOVER
DHCP OFFER
DHCP REQUEST
DHCP ACK
46
CCCH: CELL UPDATE
47
CCCH: CELL UPDATE CONFIRM

RÉPUBLIQUE FRANÇAISE

2842055

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FA 620418
FR 0208481

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	WO 01 17310 A (ERICSSON TELEFON AB L M) 8 mars 2001 (2001-03-08) * page 6, ligne 15 - page 12, ligne 22 * * page 13, ligne 14 - page 15, ligne 5 * * page 20, ligne 20 - page 21, ligne 2 * * page 22, ligne 3 - page 22, ligne 21; revendications 1-45; figures 1-3,9,11 *	1-21	H04L12/417
X	EP 1 161 055 A (IBM) 5 décembre 2001 (2001-12-05) resumé * alinéa '0016!; revendications 1-12; figure 4 *	1-21	
A	WO 01 06805 A (ERICSSON TELEFON AB L M) 25 janvier 2001 (2001-01-25) resumé * figures 1-3 *	1-21	
A	MURTHY U ET AL: "Firewalls for security in wireless networks" SYSTEM SCIENCES, 1998., PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON KOHALA COAST, HI, USA 6-9 JAN. 1998, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 6 janvier 1998 (1998-01-06), pages 672-680, XP010262834 ISBN: 0-8186-8255-8 * page 675, colonne de gauche, ligne 22 - page 676, colonne de gauche, ligne 21; figure 4 *	1-11	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04L

1

Date d'achèvement de la recherche	Examinateur
2 juin 2003	Schwibinger, H-P

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0208481 FA 620418

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 02-06-2003
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0117310	A	08-03-2001	AU	7047100 A	26-03-2001
			CN	1385051 T	11-12-2002
			EP	1208715 A1	29-05-2002
			WO	0117310 A1	08-03-2001
EP 1161055	A	05-12-2001	EP	1161055 A2	05-12-2001
			AU	7184300 A	30-08-2001
			JP	2001325469 A	22-11-2001
WO 0106805	A	25-01-2001	SE	514769 C2	23-04-2001
			AU	6192200 A	05-02-2001
			CN	1375173 T	16-10-2002
			EP	1195071 A1	10-04-2002
			JP	2003504773 T	04-02-2003
			WO	0106805 A1	25-01-2001
			SE	9902746 A	17-01-2001

EPO FORM P0465